UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/507,114	09/10/2004	Andrea Soppera	36-1838	4734

23117 7590 11/14/2007
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
11/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/507,114	SOPPERA, ANDREA	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 August 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 24 August 2007 has been noted and made of record.

2. Claims 1-45 have been presented for examination.

Response to Arguments

3. Applicant's amendments, filed 24 August 2007, with respect to the drawings have been fully considered and are persuasive. The objection of Figures 1-3 has been withdrawn.

4. Applicant's amendments, filed 24 August 2007, with respect to the specification have been fully considered and are persuasive. The objection of the specification has been withdrawn.

5. Applicant's amendments, filed 24 August 2007, with respect to claims 38-45 have been fully considered and are persuasive. The 35 U.S.C. 112, 2ND paragraph rejection of claims 38-45 has been withdrawn.

6. Applicant's arguments with respect to the prior art rejection of claims 1-45 have been considered but are moot in view of the new grounds of rejection set forth below.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 22-37 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. Claims 22-37 are directed toward a key distribution system, but fail to recite any structural elements that would comprise the system. In fact, the claim limitations of claim 22 amount to nothing more than nonfunctional descriptive data.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 1-16 and 21-45 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 6,240,188 B1 to Dondeti et al., hereinafter Dondeti.

11. As per claims 1 and 21, Dondeti teaches a method and system of managing keys in a key distribution system for a communications group, the key distribution system maintaining a tree of nodes including at least one leaf node that has a parent node, each node of the group being associated with a first key, the method comprising:

updating the first keys of a first branch of nodes in the tree by allocating new first keys to each of the nodes in the branch (column 3, lines 47-63, i.e. updating keys on a branch when a member join or leaves);

determining an offset (i.e. binary ID) for generating the updated first key of each node in the branch from a key of a previous node in the branch (column 3, lines 29-48, column 4, lines 22-65, i.e. neighbors are responsible for distributing/updated binary IDs to new members); and

broadcasting each of said offsets in an unencrypted form so that, given the updated first key associated with the first node of said branch, each updated first key of said branch of nodes can be calculated (column 6, lines 22-43, i.e. broadcasting membership updates).

12. Regarding claims 2 and 43, Dondeti teaches wherein the first key of each parent node in said tree of nodes is generated from the first key of each of its child nodes by two one-way functions (column 4, lines 7-51) and a mixing function (Figure 1 [block 34], column 4, lines 19-21, column 4, lines 61-65), the mixing function including the offset as a parameter (column 3, lines 29-48, column 4, lines 22-65).

13. With regards to claims 3, 23, and 44, Dondeti teaches wherein the mixing function in an XOR function (column 4, lines 61-62).

14. With regards to claims 4, 24, and 45, Dondeti teaches wherein each parent key is generated using the formula f(f (child key) XOR OFFSET) (igure 1 [block 34], column 4, lines 19-21, column 4, lines 61-65), wherein OFFSET is the offset and f represents a one-way function (column 4, lines 7-51) and wherein child key is the first key of a child node of said parent node (column 4, lines 19-21, column 4, lines 61-65).

15. Regarding claims 5, 26, and 39, Dondeti teaches wherein the communication group comprises at least one member that is associated with a leaf node of the tree of nodes (column 3, lines 19-28).

16. With regards to claims 6 and 27, Dondeti teaches wherein information transferred to, from or between members of the communication group is encrypted using an application data encryption key, the encryption key comprising a join field and a leave field, wherein each

member of the group knows the join field of the encryption key (column 3, lines 34-40, column 3, lines 58-63, column 6, lines 20-42).

17. Concerning claims 7, 28, and 40, Dondeti teaches wherein the join field of the encryption key is updated each time a member joins the group (column 3, lines 58-63, column 6, lines 20-42).

18. Concerning claims 8 and 29, Dondeti teaches wherein the new member joins the group using the following method:

the new user requests access to the group (column 3, lines 34-40);

the new user is granted access to the group (column 3, lines 34-40);

the new member is assigned a node at a new leaf node of the communication group (column 3, lines 29-47);

the new member is sent all the information required to generate the first key of each node on a branch of nodes from the new leaf node to the root node (column 3, lines 29-47); and

the join field of the application data key is updated (column 6, line 20 to column 8, line 13).

19. Concerning claims 9 and 30, Dondeti teaches the generation of a new node as the parent of both the new leaf node and a pre-existing node (Figure 5, column 5, lines 36-67, column 9, line 66 to column 10, line 11, column 10, lines 29-39).

20. Concerning claims 10, 31, and 41, Dondeti teaches wherein the updated join field is generated from the previous join field using a one-way function (column 4, lines 7-11, column 6, line 20 to column 8, line 13).

21. Concerning claims 11, 32, and 42, Dondeti teaches wherein a key update request is generated each time a member leaves the group, wherein the first keys of each node of the branch of nodes including both the node associated with the member that is leaving the group and the root node are the keys that are updated (column 3, lines 58-61, column 8, line 44-67).

22. Concerning claims 12 and 33, Dondeti discloses wherein a member leaves the group using the following method:

an instruction to remove a member from the group is generated (column 8, line 55 to column 9, line 19);

the parent node of the node associated with the leaving member is deleted (column 8, line 55 to column 9, line 19);

the sibling node of the node associated with the leaving member is promoted to the position occupied by the deleted node (column 8, line 55 to column 9, line 19);

the first key of each node on the branch of nodes from the promoted node to the root node is updated (column 3, lines 47-63, column 4, lines 1-21);

offset messages for generating the new first keys are broadcast to the group (column 6, lines 22-43, i.e. broadcasting membership updates);

remaining members of the communications group calculate the updated first key nodes of the tree (column 4, lines 22-65, column 5, lines 36-67).

23. Concerning claims 13 and 34, Dondeti teaches wherein the instruction to remove a member from the group is generated by the member that is leaving the group (column 8, line 55 to column 9, line 19).

24. Concerning claims 14 and 35, Dondeti teaches that the instruction to remove a member from the group is generated by a key distribution server (column 1, lines 58-66, column 8, line 55 to column 9, line 19). Evictions from a key distribution server are well-known and commonly practiced.

25. Regarding claims 15 and 36, Dondeti teaches wherein the nodes are arranged in a hierarchical tree (column 3, lines 64-65).

26. With regards to claims 16 and 37, Dondeti teaches wherein the nodes are arranged in a binary tree (column 3, lines 64-65).

27. As per claim 22, Dondeti teaches a key distribution system for a communications group, the key distribution system maintaining a tree of nodes including at least one leaf node that has a parent node, each node being associated with a first key, wherein:

the first key of each parent node in the tree is derived from the first key of each of its child node by two one-way functions (column 4, lines 7-51) and a mixing function (Figure 1 [block 34], column 4, lines 19-21, column 4, lines 61-65), the mixing function including an offset value as a parameter which is broadcast in an unencrypted form (column 3, lines 29-48, column 4, lines 22-65, column 6, lines 22-43).

28. Regarding claim 25, Dondeti teaches wherein the first keys of a first chain of nodes along a branch of the tree are updated by allocating new first keys to each of those nodes in response to a request to update the first keys of that chain of nodes (column 3, lines 47-63, i.e. updating keys on a branch when a member join or leaves);

an offset for generating the updated first key of each member of the chain from the previous member of the chain is determined (column 3, lines 29-48, column 4, lines 22-65, i.e. neighbors are responsible for distributing/updated binary IDs to new members); and

each of said offsets is broadcast so that, given the updated first key associated with the first node of said chain of nodes, each updated first key on said chain of nodes can be calculated (column 6, lines 22-43, i.e. broadcasting membership updates).

29. As per claim 38, Dondeti teaches key distribution system for a communications group, the key distribution system comprising:

an encryption key distribution server including means for maintaining a tree of nodes including a root node that has at least one child node, and at least one leaf node that has a parent

node (Figures 1, 2, 3, and 4 [blocks 54], column 1, lines 58-66, column 3, lines 19-28, column 8, line 55 to column 9, line 19),

the distribution server including means for servicing a communication group comprising at least one member client device, wherein a served encryption key defined in a server memory device comprises a join field and a leave field, and wherein:

each member client device of the group knows the join field of the encryption key (column 4, lines 7-11, column 6, line 20 to column 8, line 13);

each node of the key distribution system is associated with a leave key (Figure 8, column 8, lines 44-67);

the leave field of the encryption key is derived from the leave key of the root node (Figure 8, column 8, lines 44-67).

Claim Rejections - 35 USC § 103

30. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

31. Claims 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dondeti.

32. Regarding claim 17, Dondenti does not teach retransmitting messages enabling, users to update keys in case the users have not received those messages.

33. One of ordinary skill in the art could have tried to retransmit the messages to those users that did not receive the update at the time the invention was made, since it would provide a method for ensuring that all members of the group update their respective key.

34. With regards to claim 18, Dondeti does not teach wherein the retransmitted messages are attached to application data packets.

35. One of ordinary skill in the art could have tried to retransmit the messages attached to data packets at the time the invention was made, since it would minimize the amount of network traffic.

36. With regards to claim 19, Dondeti teaches wherein the retransmitted messages contain a sequence number indicative of the position in the sequence of key updates (column 3, lines 29-48, column 4, lines 22-65, i.e. binary ID).

37. Concerning claim 20, Dondeti teaches wherein the sequence number is cyclic (column 3, lines 29-48, column 4, lines 22-65, i.e. the binary ID is cyclical).

Conclusion

38. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

39. The following patents are cited to further show the state of the art with respect to key management, such as:

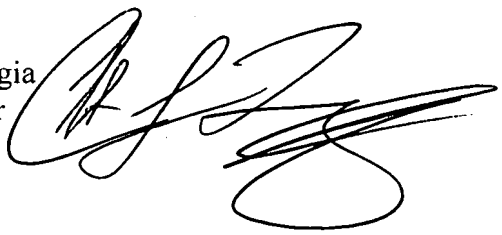
United States Patent No. 7,095,850 B1 to McGrew, which is cited to show updating a key tree using offsets.

40. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

41. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

42. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131



clf